

MAC105 FUNDAMENTOS DE MATEMÁTICA PARA A COMPUTAÇÃO

FOLHA DE SOLUÇÃO

Nome: PEDRO GIGEL FREIRE

Número USP: 10737136

Assinatura

PEDRO GIGEL FREIRE

Sua assinatura atesta a autenticidade e originalidade de seu trabalho e que você se compromete a seguir o código de ética da USP em suas atividades acadêmicas, incluindo esta atividade.

Exercício: E63

Data: 20/06/18

SOLUÇÃO

SABEMOS QUE $aR = \{ar : r \in R\}$ tem o mesmo número de elementos que R . PARA SER UM SISTEMA COMPLETO DE RESÍDUOS, TODOS OS ELEMENTOS DE aR PRECISAM SER DE CLASSES DE CONGRUÊNCIA MÓDULO p DISTINTAS.

ISTO É, SE PEGARMOS DOIS ELEMENTOS ARBITRÁRIOS x E x' DE aR , DEVEMOS TER QUE $x \not\equiv x' \pmod{p}$.

SEJAM $x = ar$, $x' = ar'$, $r \neq r'$, VAMOS SUPOR, POR ABSURDO, QUE $x \equiv x' \pmod{p}$. ENTÃO $ar \equiv ar' \pmod{p}$. SEGUE QUE $p \mid ar - ar' \Rightarrow p \mid a(r - r')$. COMO $p \nmid a$, ENTÃO $p \mid r - r'$, OU SEJA, $r \equiv r' \pmod{p}$.

MAS ISSO É UMA CONTRADIÇÃO, POIS r E r' PERTENCEM A R , UM SISTEMA COMPLETO DE RESÍDUOS, ENTÃO r NÃO É CONGRUENTE MÓDULO p A r' .

PORTANTO, $x' \not\equiv x \pmod{p}$ E aR É UM SISTEMA COMPLETO DE RESÍDUOS.